災害と AI サイバー攻撃の二重リスクに備える。
～いま、企業に求められる統合型セキュリティとは。～

クラウドソリューション事業本部
第一技術部　チーフ IT アーキテクト
河野 大悟 / KONO DAIGO

システセキュリムエンジニアとして 20 年従事。エンタープライズ、自治体、文教のネットワーク、クラウド、セキュリティ案件のプロジェクトマネージャ経験。Microsoft 認定資格の Azure Cyber Security Architect Expert など複数の資格保持。2025 年 Microsoft Top Partner Engineer Award Security カテゴリ受賞。

【専門領域】
・AI 活用の進展を踏まえたセキュリティ動向
・Microsoft Azure を活用した実践的セキュリティ強化
・事業継続を見据えた IT-BCP ／ DR 設計
・セキュリティと利便性を両立するシステム設計

すべての工程で高い水準を追求

近年、大手企業のサイバーインシデントによる業務停止を受け、日本企業はセキュリティ対策に本格的に取り組む必要に迫られています。

多くのお客様が「何から始めればいいかわからない」という状態にあります。私たちは単一製品ではなく、システム全体のアーキテクチャを設計するアプローチを大切にしています。この提案姿勢を一貫して続け、Microsoft ソリューションを中心に設計してきたことが、今回のアドバンスドスペシャライゼーション取得につながりました。

私たちが特にこだわっているのは、セキュリティソリューションをサイロ化しないこととセキュリティと利便性のバランスです。製品をバラバラに導入するとシステム全体を把握できなくなるため、サイロ化を避け、ユーザーの運用負担を最小化しながらセキュリティを強化します。

セキュリティインシデントには、外部攻撃（ランサムウェアなど）、内部要因（内部不正や誤操作）、システム要因（設定不備や脆弱性）という三つの観点があります。多くのお客様は外部攻撃のみに注目しがちですが、実際には 3 つすべてが重要です。

お客様が認識している顕在課題だけでなく、潜在課題にも目を向け、「実はここがより重要です」という気づきを提供することが私たちの役割です。私たちにとってセキュリティとは、単に攻撃を防ぐ仕組みではなく、お客様の事業を止めないための設計です。

バーチャル環境全体で可用性を確保する

今回、Microsoft Azure のセキュリティ強化に関する専門的で有益な活用事例が評価されましたが、私が手がけた事例の中でも特に難易度が高かったのが、ある大手製造業企業の IT-BCP 実装プロジェクトです。

本案件では、災害対策（DR）とセキュリティ事故対策という 2 つの重要な要件を同時に満たす必要がありました。東日本で大規模災害が発生した場合には西日本へ切り替えられる構成とするとともに、セキュリティ事故発生時にも迅速に復旧できる仕組みを整備することが求められました。これらは、当社と Microsoft の知見を組み合わせることで実現したものです。Azure Site Recovery、Azure Backup、Azure Virtual WAN を活用し、災害対策を踏まえた論理的な WAN 構成を構築しました。

お客様はもともと Azure 東日本リージョンで基幹システムを稼働させており、拠点ネットワークも東日本リージョンのみに接続されている構成でした。そのため、DR を実現するためには、仮想環境と実際の拠点ネットワークの両方を含めた構成の見直しが必要でした。そこで Azure Virtual WAN を活用し、各主要拠点を Azure に接続したうえで DR 構成を構築しました。各拠点を Azure Virtual WAN に接続し、拠点ネットワークも含めた DR 構成を実現する事例は国内でもまだ多くなく、我々の強みの一つになったと感じています。

当社が持つネットワーク設計の知見と、Microsoft のクラウドアーキテクチャの知見を組み合わせることで実現したものだと思っています。

お問合せ
経営企画部 広報担当 白木
TEL: 050-1781-1448 E-mail: pr-info@sojitz-ti.com

――災害対策と AI セキュリティ対策の両立

個々の拠点を守るのではなく、システムをバーチャル環境上で稼働できるようにし、障害発生時には機能を別の拠点へ移せる体制を構築する考え方です。

今回の案件は、物理的な障害への対応やネットワーク構成など、非常に複雑でした。加えて、ランサムウェア対策も重要な要素でした。攻撃を受けたシステムの復旧に備え、イミュータブルバックアップ（不変性を持たせた設計）や、東日本で取得したバックアップを西日本で起動させる「クロスサイトリカバリ」を採用しました。

BCP の観点だけでなく、サイバー攻撃への対策もますます重要になっています。ランサムウェアはもちろん、最近では AI を活用した攻撃も増えており、攻撃の巧妙化と被害の深刻化が進んでいます。従来のクラウドセキュリティとは異なる視点での対策が必要です。

攻撃側も防御側も、すでに AI を活用する流れが始まっています。例えば、Microsoft Defender for XDR は、エンドポイント、メール、ID など複数のセキュリティ領域の情報を統合し、AI で脅威を検知・分析します。Microsoft Sentinel のような SIEM と組み合わせることで、ログ分析から検知、対応までをより高度に自動化できます。AI が脅威を検出し、分析し、必要に応じて自動対応する。こうした仕組みは今後さらに普及していくでしょう。

私たちは、こうした最新のソリューションを活用しながら、AI 時代のセキュリティに対応していきます。Defender for XDR や Microsoft Sentinel といった最新技術を取り入れ、チーム全体で知識を高め、成長し続けられる環境を築いていきたいと思っています。

――― AI 時代に求められる人間の設計力

防衛側も攻撃側も AI 対 AI になってくる中で、人間の設計力や可能性はどこで問われるようになるのか。

当社 クラウド事業本部 第一技術部メンバー

まず重要なのは、AI は使う人間次第だということです。AI が自動的にすべてを守ってくれるわけではなく、お客様の環境に合わせてどのように動かすか、どのように設計するかが非常に重要になります。人がチューニングしていく部分もありますし、その環境に適した設定を行うことも必要です。そういった部分を評価するアセスメントやコンサルティングには、今後も人の力が不可欠だと考えています。単純に AI が自己防衛してくれるから安心というわけではありません。お客様の環境に応じて AI の強度や設定を調整する必要があります。それによって使い勝手も大きく変わりますし、設定を誤れば逆に運用に影響が出ることもあります。

最終的には、こうした調整の手間は AI によってかなり自動化されていくと思います。ただ、現在はまだ過渡期であり、人が環境に合わせて調整していく段階にあると言えると思います。

実際、AI の進化は非常に速く、１年前と比べても大きく変わっています。精度も速度も、半年前と比べて大きく向上しています。

AI 対 AI のセキュリティの世界で、どの時点で人間が追いつけなくなるのかを正確に予測することは難しいですが、私は比較的早い段階でそうした状況になる可能性があると考えています。

すでに AI が自動的に通信を分析し、通常とは異なるパターンを検出した場合に即座にブロックするといった機能を持つソリューションも登場しています。そうした意味では、AI 対 AI の時代は決して遠い未来ではなく、すでに始まっていると言えるのかもしれません。

■双日テックイノベーションについて
社名：双日テックイノベーション株式会社
所在地：東京都千代田区二番町３-５麹町三葉ビル（受付６F）
設立：1969 年２月 24 日
URL：https://www.sojitz-ti.com/
国内外の最新ソリューションによるネットワーク・IT インフラ構築、システム開発、運用・保守などのサービス提供、およびデジタルトランスフォーメーション支援。

お問合せ
経営企画部 広報担当 白木
TEL: 050-1781-1448 E-mail: pr-info@sojitz-ti.com